REMARKS

This is in response to the Office Action mailed on November 19, 2004, and the references cited therewith.

Claims 1, 2, 12 and 14 are amended, no claims are canceled, and claims 34-36 are added; as a result, claims 1-36 are now pending in this application.

§102 Rejection of the Claims

Claims 1-2, 12, 14, 20, 21, 28 and 32-33 were rejected under 35 USC § 102(b) as being anticipated by Lei Tang (Method for Encrypting and Decrypting MPEG Video Data Efficiently) recited in the IDS, paper number 4 by Applicant.

§103 Rejection of the Claims

Claims 3-6, 13, 15-17 19, 22-23 and 25 were rejected under 35 USC § 103(a) as being unpatentable over Lei Tang (Method for Encrypting and Decrypting MPEG Video Data Efficiently) recited in the IDS, paper number 4 by Applicant in view of Rhoads (U.S. 6,567,533 B1).

Claims 1,12

The amendments to claims 1 and 12 are based on Fig. 1A and on page 3, lines 14-22 of the application as filed. Thus, no new subject-matter has been added. In particular, Fig. 1A shows that scrambler 9 performs a scrambling operation on the signal received on input 4, which takes the scrambling control information based on the output of analyser 3 as input (in addition to a secret key).

Novelty

The subject-matter of claims 1 and 12 is novel compared with Tang, L., "Method for Encrypting and Decrypting MPEG Video Data Efficiently", *Proc. of ACM Multimedia 96*, Boston,

Nov. 1996, p. 219-229 (hereinafter referred to as D1), because D1 does not disclose scrambling means receiving the information signal as input and arranged to perform a scrambling operation on the information signal controlled by the information on the entropy distribution received as input from the analysing means. Instead, in the system known from D1, quantized DCT coefficients are received as input by the scrambling means, as well as a 1 × 64 permutation list (page 223, right-hand column, first ten lines). The original information signal from which the DCT coefficients were obtained is not an input to the scrambling means.

The subject-matter of claims 1 and 12 is novel compared with US 6,567,533 (hereinafter referred to as D2), because D2 does not disclose scrambling means providing a scrambled information signal having an entropy distribution corresponding to that of the original signal. Instead, scaled noise signal samples are added to input signal samples (column 17, lines 9-10). As is clear from column 19, lines 19-32, the addition changes the entropy distribution of the signal.

Obviousness

The subject-matter of claims 1 and 12 differs from D1 in that D1 does not disclose scrambling means receiving the information signal as input and arranged to perform a scrambling operation on the information signal controlled by the information on the entropy distribution so as to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal. Instead, the known scrambling means receive an 8 × 8 block of DCT coefficients and use a random permutation list to replace the zig-zag order thereof to map the 8 × 8 block to a 1 × 64 vector. The goal is to achieve compression and encryption in one step (page 223, right-hand column, first line).

The effect of this difference is that compression and scrambling are inseparable. The manner of scrambling dictates the type of compression. This is the case, because the scrambling method relies on the use of a Discrete Cosine Transform on the original information signal,. an analysis of the entropy distribution. The present invention, by contrast, provides a system for processing an information signal and system for scrambling an information signal that allows all stages of a

compression algorithm to take place subsequent to the scrambling, so as to reduce the possibility of even a partially compressed original information signal being present in the clear. The objective problem solved by the invention as defined in claims 1 and 12 is thus to provide systems allowing a complete separation of the scrambling and compression steps, to allow all compression to be carried out subsequent to scrambling as a manner of improving protection against unauthorised copying of the information signal.

The solution to this problem is not to be found in D1, which teaches away, insofar as it relates to a system for achieving compression and encryption in one step.

The skilled person faced with the problem outlined above has no incentive to combine the teachings of D1 and D2, because D2 relates to the field of watermarking (column 1, lines 40-45). Furthermore, D2 does not disclose scrambling means receiving information on the entropy distribution of the information signal and the information signal as input which are arranged to perform a scrambling operation on the information signal controlled by the information on the entropy distribution. Instead, D2 only discloses the use of any of dozens of well known scrambling methods (column 33, lines 48-50).

As a secondary indication of the inventive character of the invention defined in claims 1 and 12, it is observed that the invention is based on the recognition of a previously unrecognised problem, as well as providing effects not attainable by the techniques known from the prior art. In particular, D1 fails to recognise that, whilst it would be desirable not to carry out compression prior to encryption, separation of the two processes is desirable to achieve versatility in the choice of compression algorithm. The incorporation of this inventive insight allows a broader range of application of the present invention compared with the prior art. The most appropriate compression algorithm, including lossy algorithms, can thus be employed.

Claim 2

The amendment to claim 2 finds basis in the description, page 4, lines 14-22 of the application as filed.

The subject-matter of claim 2 is novel and non-obvious because claim 2 relates to a system having all features of a system according to claim 1. The same holds true for claims 3-11.

Claim 13

The subject-matter of claim 13 is novel and involves an inventive step, because claim 13 relates to a system according to claim 12.

Claim 14

Claim 14 has been amended, relative to the version currently pending, by specifying that the scrambling signal is re-generated as a descrambling signal under the control of information representative of the entropy distribution of the information signal. Basis for this feature is provided on page 5, lines 1-2 of the application as filed. Thus, the subject-matter of claim 14 is not extended unduly.

In response to the Examiner's remark on page 3 of the latest Office Action, it is observed that the feature 'obtainable by combining a scrambling signal with the information' should be given patentable weight.

"[A] claim preamble has the import that the claim as a whole suggests for it." *Bell Communications Research, Inc. v. Vitalink Communications Corp.*, 55 F.3d 615, 620, 34 USPQ2d 1816, 1820 (Fed. Cir. 1995). "If the claim preamble, when read in the context of the entire claim, recites limitations of the claim, or, if the claim preamble is 'necessary to give life, meaning, and vitality' to the claim, then the claim preamble should be construed as if in the

balance of the claim." *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305, 51 USPQ2d 1161, 1165-66 (Fed. Cir. 1999). It is submitted that the preamble does in fact give life, meaning, and vitality' to the claim and, accordingly, the claim preamble should be construed as if in the balance of the claim. It is also not correct to state that the body of claim 14 does not depend on the preamble for completeness, because claim 14 further includes the feature 'means for regenerating the scrambling signal'. Thus, the latter feature relies on the former for antecedent basis.

Novelty

The subject-matter of claim 14 is novel compared with D1, because D1 does not comprise means for regenerating the scrambling signal as a descrambling signal under the control of information representative of the entropy distribution of the information signal. Instead, D1 discloses that scrambling is carried out by using a random permutation list to replace the zig-zag order to map an 8 × 8 block of DCT coefficients to a 1 × 64 vector. The secret key is the 1 × 64 permutation list. Thus, to decrypt the scrambled compressed information signal using the methods of D1, a descrambling signal comprising a permutation list to map the 1 × 64 vector back to the 8 × 8 block is needed, in addition to the scrambled compressed information signal itself. D1 thus does not disclose regenerating the scrambling signal as a descrambling signal, much less doing so under the control of information representative of the entropy distribution of the information signal.

Note has been taken of the Examiner's remark on page 7, regarding the disclosure in section 3 of D1. It is observed firstly that section 3 of D1 is entitled 'related works'. It does not relate to the combined encryption and compression algorithm that is the focus of D1. "Anticipation requires the presence in a single prior reference disclosure of each and every element of the claimed invention, *arranged as in the claim.*" *Lindemann Maschinenfabrik GmbH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 221 USPQ 481, 485 (Fed. Cir. 1984) (citing *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 220 USPQ 193 (Fed. Cir. 1983)) (emphasis added). Secondly, if one were to regard the sequence of I-frames as the descrambling signal, with

the P- and B-frames being the information signal, then selective encryption does not involve the use of means for regenerating the scrambling signal as a descrambling signal under the control of information representative of the entropy distribution of the information signal, because entropy information relating to the P- and B- frames is not used to recover the I-frames.

The subject-matter of claim 14 is novel compared with D2, because D2 does not disclose means for regenerating the scrambling signal as a descrambling signal under the control of information representative of the entropy distribution of the information signal. In fact, D2 does not disclose in any detail the descrambling means employed. Instead, it is merely noted that 'any of dozens of well known scrambling methods' may be used, so that, presumably, any of dozens of corresponding descrambling methods would also be used.

Obviousness

The subject-matter of claim 14 is not obviously suggested by D1 and D2, either. The subject-matter of claim 14 differs from the system known from D1, because D1 does not disclose descrambling means comprising means for regenerating a scrambling signal as a descrambling signal under the control of information representative of the entropy distribution of the information signal (see above with respect to 'novelty').

The effect of this difference is that the system defined in claim 14 efficiently allows complete decompression prior to descrambling of a compressed scrambled signal, by combining the decompressed scrambled information signal with a descrambling signal adapted not to effect significantly the entropy distribution of the signal. Thus, the objective problem solved by the system according to claim 14 is to provide such a system.

The system defined in claim 14 solves the objective problem, because it allows a descrambling signal to be generated in dependence on the entropy distribution of the scrambled information signal in uncompressed form, on the basis of the information representative of the entropy distribution. Additionally, implementation is efficient, because the presence of the means for

regenerating the scrambling signal as a descrambling signal means that only the information representative of the entropy distribution need be provided, instead of an entire copy of the scrambling signal.

The skilled person seeking to find a solution to the objective problem outlined above would not turn to D2, because D2 relates to watermarking and decoding a watermark present in a compressed scrambled signal (column 1, lines 43-45). Even were the skilled person to turn to D2, he would find no suggestion of means for regenerating a scrambling signal under the control of information representative of the entropy distribution of the information signal. Instead, D2 only discloses recovering a watermark from a scrambled signal, without going into the type of descrambling process.

Thus, the invention defined in claim 14 is not obviously derivable from the cited prior art. Furthermore, the invention provides effects not achievable using prior art methods, such as those known from D1 for instance. The invention allows a complete separation of the descrambling and decompression operations in a system for processing scrambled compressed information signals. Thus, a greater choice of compression algorithms is available. Moreover, because the descrambling system regenerates the scrambling signal using the information representative of the entropy distribution, the scrambling signal can be varied rapidly without having to provide it in full to the descrambling system. This further increases the security of the system. In the system of D1, such variation is only attainable by varying the key (the permutation list), which has to be made available to the descrambling system.

Claims 34, 36

Claims 34 and 36 are based on claim 7 of the application as filed, as well as on page 4, lines 34-37 and page 3, lines 13-14 of the application as filed. Thus, claims 34 and 36 are fully supported by the contents of the application as filed.

Claim 35

Claim 35 is supported by the passage on page 3, lines 27-28 of the application as filed.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at 408-333-9972 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

ANDREW AUGUSTINE WAJS ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-333-9972

Date 01/27/05 By _____
Andre L. Marais
Reg. No. 48,095

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 27th day of January, 2005.

Dawn R. Shaw _____
Name Signature